Health Insurance Portability and Accountability Act (HIPAA)

Utah Department of Health
Division Of Health Care Financing
Initial Security Awareness Training

HCF Security Training Version 1.1
March 21, 2005

Working Together!

HIPAA Overview

- **Intended to improve "the efficiency and effectiveness of health information systems through establishment of standards and requirements for the electronic transmission of health information"**

- **Establishes Federal regulation of:**

  - **Transactions and Code Sets**
  - **Health care identifiers**
  - **Confidentiality health information (Privacy)**
  - **Security of electronically maintained/communicated health information (Security)**

Security Objective

- **To minimize the risk of intentional or accidental disclosure or misuse, or the loss or corruption of individually identifiable health information (IIHI)***

***IIHI - Any information, including demographic information collected from an individual that a) is created or received by a health care provider, health plan, employer, or health care clearing house; and b) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual, or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.**

Why HIPAA?

- **Some members of the Division of Health Care Financing workforce come in contact with protected health information (PHI) and provider/payer identifiers and other security related information in the completion of their duties on behalf of Division of Health Care Financing**

- **This document enhances the HR Manual and documents HIPAA policies that are guidelines to help safeguard PHI and other information from being used by those who are not authorized**

- **Division of Health Care Financing's guidelines and policies are the rules we must apply while at the same time attempting to safeguard even the potential that PHI may be inadvertently divulged**

General Guidelines

- **Division of Health Care Financing personnel will reasonably safeguard PHI to limit incidental uses or disclosures**
- **An incidental use or disclosure is a secondary use disclosure that cannot reasonably be prevented**
  - **Is generally limited in nature and that occurs as a by-product of an otherwise permitted use or disclosure**
- **All members of the Health Care Financing workforce will follow these guidelines in handling PHI or other security related identifiers to limit incidental uses and disclosures**

Safeguard Guidelines

Cleaning Personnel

- **Whenever reasonably possible, PHI should be placed in locked containers, cabinets, or out of sight (covered or face down on counters or desks)**

Computer Screens

- **Computer screens at each workstation should be positioned so that only authorized user at that workstation can read the display**
- **Computer displays will be configured to go blank, or to display a screen saver, when left unattended for more than a brief period of time**
- **Computer screens left unattended for longer periods of time should be logged off by the user**

Safeguard Guidelines

Conversations

- **Conversations concerning individual care, PHI, or security information such as ID's or passwords or other methods of authentication must be conducted in a way that reduces the likelihood of being overheard by others**

Copying PHI Information or Reports

- **When PHI or identifier are copied, only the information that is necessary to accomplish the purpose for which the copy is being made, may be copied**

- **This may require that part of a page be masked (blacked out)**

Safeguard Guidelines

Desks and Countertops

- **Provider reports and other documents which may display identifiers and other "keys" to information should be placed face down on counters, desks, and other places where individuals or visitors can not see them**
- **Wherever it is reasonably possible to do so, documents containing PHI will not be left on desks and countertops after business hours**
- **In areas where locked storage after hours cannot reasonably be accomplished, PHI and security related identifiers must be kept out of sight**

Safeguard Guidelines

Disposal of paper with PHI or Identifiers

- Paper documents containing PHI must be shredded when no longer needed
- If retained for a commercial shredder, they must be kept in a locked bin

Home Office

- Any member of the workforce who is authorized to work from a home office must assure that the home office complies with all applicable policies and procedures regarding the security and privacy of PHI, including these guidelines

Safeguard Guidelines

Facility Access and Key Policy

- **The Security and Privacy Officers will develop a list of which personnel, by job title, may have access to which keys. This includes access to storage cabinets, storage rooms and buildings**
- **All keys must be signed out and surrendered upon termination of employment**
- **The Security Officer will act to change locks whenever there is evidence that a key is no longer under the control of an authorized member of the workforce, and its loss presents a security threat that justifies the expense**

Safeguard Guidelines

Transporting of PHI Information

- **When a member of the workforce is transporting PHI from one building to another, it may not be left unattended unless it is in a locked vehicle, in an opaque, locked container**
  - **Locking the vehicle alone is not sufficient**

Record Storage

- **Areas where records and other documents that contain PHI are stored must be secure.**
  - **Wherever reasonably possible, use locking cabinet**
  - **Where locking cabinets are not available, the storage area must be locked when no member of the workforce is present to observe who enters and leaves and no unauthorized personnel may be left alone in such areas without supervision**

Safeguard Guidelines

Personal Digital Assistants (PDA) and Laptops

- **Division of Health Care Financing privacy and security policies apply to any PHI that is stored on a PDA or LAPTOP**
- **Users of PDA and/or Laptops are responsible for assuring that their devices are kept secure and private**
- **Any loss or theft of a PDA or Laptop thought to contain PHI must be reported to the Security Officer immediately**

Visitors

- **Visitors to areas where PHI is being used must be accompanied at all times by a member of the Division of Health Care Financing workforce**

Safeguard Guidelines

Printers and Fax Machines

- **Printers and fax machines should be located in secure areas when available, where only authorized members of the workforce can have access to documents being printed**
- **Protected or sensitive information, when printed to a shared printer, should be retrieved immediately**

Workforce Vigilance

- **All members are responsible to watch for unauthorized use or disclosure of PHI, to act to prevent the action, and to report suspected breaches of privacy and security policies to their supervisor or Security Officer**

Workforce Policies

Password Standard

User IDs and passwords protect the integrity of information, provide authentication, control access, and establish user audit capabilities within the State of Utah computing environment and information resources. The combination of a user ID and password provide individual user validation that the person is authorized to access the system or device. Any individual accessing a State of Utah information resource, including employees, contractors, and vendors, is responsible for taking the appropriate steps to select and secure their passwords.

Workforce Policies

Password Policy

- **When possible, all user level passwords should be changed at least every 90 days.**
- **After three consecutive unsuccessful password attempts a user ID will be revoked or disabled until reinstated or removed by the agency security administrator.**
- **Screen savers with passwords should be used on all computers (servers, laptops, workstations) and activated after no more than 15 minutes of inactivity.**
- **Employees should password lock their screens when leaving workstations unattended.**
- **All supervisor-level passwords (e.g., root, enable, NT administration, and privileged accounts) should be changed on a regular basis, or, at minimum, every 45 days.**

Workforce Policies

Strong Passwords Characteristics

- **A password should be at least eight alphanumeric characters long.**
- **A password should not be a word in any language, slang, dialect, jargon, etc.**
- **When possible, passwords should have a combination of numeric digits and special characters, as well as lower and upper case letters.**
- **Passwords should include three of the following four attributes:**
  - **One Upper Case Character**
  - **One Lower Case Character**
  - **One Numeric Character**
  - **One Special Character**
- **Passwords should not be based on personal information, names of family members, pets, etc.**
- **When changing a password it is not acceptable to simply add a number to the end of the previous used password. For example password1, password2, etc.**

Workforce Policies

Password Protection Standards

- **Passwords should never be sent in clear text over the network. This includes email, chat, instant messaging, or any other non-secure form of information transfer.**
- **Passwords should never be stored in unsecured places, such as written down on a sticky note or saved unprotected on-line.**
- **Passwords used for the State of Utah computing environment and information resources should be different than those used for personal accounts (e.g., a personal ISP account, option trading, benefits, etc.).**
- **User IDs and passwords should never be shared with anyone, including administrative assistants, coworkers, family members, a local network administrator, your boss, or secretaries.**
- **All passwords should be treated as sensitive, confidential State of Utah information.**
- **Security and network administrators should never ask you to divulge your password.**

Workforce Policies

If a Password or User ID is Compromised

At any time a user ID or password is suspected of being compromised, the password should be changed immediately, or the account disabled

Workforce Policies

Sanctions for Violating Privacy and Security Policies and Procedures

- **Members of the Division of Health Care Financing workforce are subject to disciplinary action for violation of policies and procedures**
- **Violations that jeopardize the privacy or security of PHI or Security identifiers are particularly serious**
- **This seriousness will be reflected in the nature of the disciplinary action, up to and including termination of employment**

Workforce Policies

Sanctions for Violating Privacy and Security Policies and Procedures

- **All members of the workforce will be treated fairly and equitably in the imposition of sanctions for privacy and security violations**
- **Sanctions will be integrated into Division of Health Care Financing's overall employee discipline policy. This policy will be in writing**
- **Disciplinary actions due to breaches of privacy or security of PHI will be documented, and the documentation must be retained for seven years. Disclosure of PHI in violation of policy is reportable under the accounting of disclosures of protected health information policy**
- **No member of the workforce will be subject to sanctions for a disclosure of PHI made in good faith in accordance with the whistle blowers or victims of crime policy**

Workforce Policies

Termination or Modification of Access to Protected Health Information: Electronic Systems

- **Division of Health Care Financing will terminate access to information systems and other sources of protected health information (PHI), including access to rooms or buildings where PHI is located, when an Division of Health Care Financing employee, agent or contractor ends his/her employment or engagement**

- **Division of Health Care Financing will terminate access to specific types of PHI when the status of any member of the workforce no longer requires access to those types of information**

Workforce Policies

Physical Access Controls

- **Division of Health Care Financing will maintain strict physical access controls to its information systems at all times and under all conditions**
- **This includes the physical security of electronic and paper data**

Work Station Use and Location

- **Division of Health Care Financing will provide secure workstations containing computer terminals with physical safeguards**
- **Secure areas where sensitive information is regularly entered or utilized**

Workforce Policies

Facsimile Machines and Protected Health Information

- **PHI may be transmitted by facsimile machine ("fax"), provided all other Division of Health Care Financing policies and procedures regarding the disclosure of PHI are observed**
- **In order to reduce the potential for misdirected faxes, frequently used destination numbers will be pre-programmed into fax machines and tested before being used to transmit PHI**
- **To further reduce the possibility of misdirected faxes, each fax machine should display a key that identifies the destination for each pre-programmed fax number**
- **When PHI is faxed to a destination number that is not pre-programmed, the fax machine operator will double check the accuracy of the number in the machine's display before sending**

Workforce Policies

Facsimile Machines and Protected Health Information

- **All fax messages will include a Confidentiality Statement within the cover sheet**
- **Fax machines that are used to transmit or receive PHI should be placed in secure locations**
- **Whenever possible, fax machines used to receive PHI will not be used regularly for other purposes.**
- **Transmittal sheets will be checked immediately after each transmission of PHI to assure that the information was sent to the correct number**
- **If an error is detected, the sender must immediately act to correct the error, and report the error, to the Division of Health Care Financing Privacy Officer**
- **Transmittal sheets will be filed with the PHI that was transmitted, to document the recipient.**

Workforce Policies

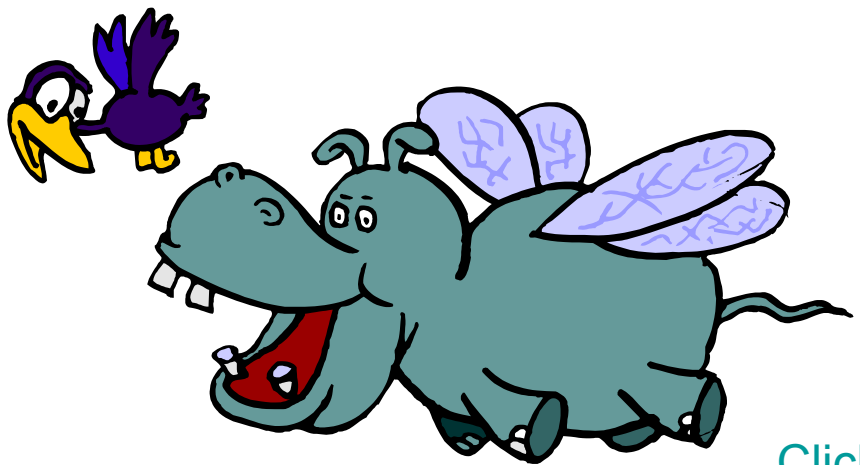
eMail and Protected Health Information

- **PHI may not be transmitted by e-mail unless the sender is using a secure e-mail system. A secure e-mail system has the following features:**
  - **The message cannot be intercepted. If the message is sent over an open network (e.g. the Internet) it must be encrypted, using an encryption standard approved by the Security Officer.**
  - **The recipient of the message will know that the content has not been altered during transmission.**
  - **The recipient of the message will know the true identity of the sender**
  - **There are safeguards to lessen the possibility of sending the message to someone who is not authorized to receive it.**
  - **There are safeguards to reduce the likelihood that the message will be forwarded to someone who is not an intended recipient.**

Workforce Policies

eMail and Protected Health Information

- **E-mail which contains PHI will not be used to transmit a message to more than one individual at one time**
- **This is to avoid the potential for inadvertent disclosure of e-mail addresses, linking e-mail addresses with clinical information in the message or violating prohibitions against using individual-specific information for certain types of marketing**



Click Here To Continue!